

Délégué à la protection des données (DPO)

RNCP41460 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	128, 326
Formacode(s)	13238, 71654
Code(s) ROME	K1903, M1802, M1806
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	27/10/2025
Date d'échéance	27/10/2028

Certificateur(s)

DORANCO ESPACE MULTIMEDIA · SIRET : 38935885400054

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le titre Délégué à la protection des données (DPO) a pour objectif d'être une réponse concrète aux besoins de compétences opérationnelles exprimés par les entreprises. Le DPO est responsable de veiller à la conformité de l'organisation au RGPD, en conseillant, contrôlant et assurant la protection des données personnelles tout en agissant comme interlocuteur auprès des autorités compétentes.

ACTIVITÉS VISÉES

Évaluation initiale de la conformité des traitements et mise à jour des registres des traitements
Encadrement des relations contractuelles et des transferts de données hors UE
Élaboration et mise en œuvre des politiques de conformité RGPD et gestion des droits des personnes concernées
Gestion des interactions avec les autorités de contrôle (CNIL)
Mise en place d'un cadre de gouvernance pour la gestion des données
Suivi des indicateurs de gouvernance et de sécurité
Supervision et suivi des audits de cybersécurité et de conformité
Gestion de la sécurité des systèmes d'information liés aux données personnelles
Réalisation d'analyses d'impact sur la vie privée (PIA)
Identification et analyse des risques de cybersécurité liés aux traitements de données
Définition et supervision des mesures de réduction des risques
Coordination des actions en cas de crise
Mobilisation et coordination des parties prenantes pour la mise en œuvre des actions RGPD
Pilotage des actions de communication internes et externes sur les enjeux de protection des données
Déploiement d'actions de sensibilisation auprès des équipes internes sur la protection des données
Formation des équipes ou collaborateurs
aux principes et procédures RGPD

COMPÉTENCES ATTESTÉES

Cartographier l'ensemble des traitements de données personnelles et sensibles de l'organisation, en identifiant les flux et les acteurs impliqués, en appliquant des techniques de classification des données selon leur sensibilité et en analysant les enjeux de conformité réglementaires et sectoriels (ex. : santé, finance, e-commerce) afin d'établir un diagnostic détaillé des flux de données et des pratiques de traitement
Évaluer la conformité des traitements existants, y compris ceux liés aux technologies émergentes, en analysant les

écarts entre les pratiques actuelles et les obligations légales et sectorielles (ex. : santé, finance, e-commerce), afin de qualifier les non-conformités et de prioriser leur gravité selon leur impact sur la conformité de l'organisation.

Produire un rapport de diagnostic détaillé, en hiérarchisant les risques identifiés (ex : risques juridiques, opérationnels, réputationnels) et en formulant des recommandations spécifiques, pour guider la stratégie de mise en conformité de l'organisation.

Créer ou mettre à jour les registres des traitements de données personnelles, en élaborant des fiches descriptives détaillées pour chaque traitement en collaboration avec les responsables métiers, en consolidant les informations requises par le RGPD (ex. : finalités, catégories de données, mesures de sécurité) et en intégrant les spécificités technologiques et métiers de l'organisation (ex. : algorithmes d'IA, protocoles IoT), afin d'assurer une traçabilité complète des activités de traitement et de garantir leur conformité aux exigences réglementaires.

Analyser les contrats en cours avec les sous-traitants et partenaires externes, en vérifiant les clauses liées à la protection des données (ex. : traitement, stockage, partage) et aux engagements des parties prenantes, en mettant en œuvre des processus d'audit contractuel afin de garantir l'application des exigences réglementaires et de sécuriser les échanges de données avec les partenaires.

Gérer les transferts de données hors Union Européenne (UE), en mettant en œuvre les mécanismes juridiques appropriés (ex. : Clauses Contractuelles Types, Binding Corporate Rules) et en assurant le suivi des obligations réglementaires, afin de garantir la conformité et sécuriser les flux transfrontaliers.

Concevoir une politique de gouvernance des données personnelles, incluant des documents opérationnels (ex. : politique de conservation des données, politique de confidentialité, charte RGPD) et des principes clés (ex. : licéité, minimisation, conservation limitée), en collaboration avec les départements métiers (ex. : juridique, IT, marketing) afin d'uniformiser les pratiques de gestion des données et de garantir la conformité au RGPD.

Concevoir des protocoles de gestion des consentements et des préférences, intégrant des mécanismes de preuve (ex : horodatage, journalisation) et de révocation (ex : interface utilisateur dédiée, processus automatisé de suppression), en veillant à leur accessibilité et leur compréhension par l'ensemble des publics concernés, y compris les personnes en situation de handicap, afin de garantir le respect des choix des personnes concernées et leur traçabilité tout au long du cycle de vie des données.

Mettre en place un processus structuré de gestion des demandes d'exercice des droits des personnes concernées (ex. : droit d'accès, droit d'effacement, droit d'opposition), en intégrant des workflows automatisés (ex. : système de ticketing), en veillant à l'accessibilité des démarches pour tous les publics, notamment les personnes en situation de handicap, et en définissant des indicateurs clés de suivi (ex. : délais de réponse, taux de résolution), afin de garantir un traitement conforme et une traçabilité des demandes dans les délais réglementaires.

Gérer les échanges avec la CNIL lors d'un contrôle ou d'une demande d'information, en rassemblant les éléments de conformité requis et en coordonnant la communication entre les parties prenantes internes et l'autorité de contrôle, afin d'assurer une coopération efficace et démontrer la conformité de l'organisation.

Cartographier les acteurs internes et externes impliqués dans la gestion des données personnelles, en identifiant leurs rôles et responsabilités afin d'assurer une gouvernance alignée avec les objectifs de conformité.

Définir un cadre de gouvernance en collaboration avec les équipes IT et juridiques pour intégrer les principes de Privacy by Design et Privacy by Default dès la conception d'un projet impliquant des traitements de données (ex : déploiement d'un SIRH, développement d'une application métier, implémentation d'une solution d'IA)

Suivre les politiques de gouvernance et de sécurité à travers des indicateurs clés de performance (KPI) (ex. : taux de résilience aux cybermenaces, conformité des sous-traitants) et des tableaux de bord, en identifiant les écarts pour optimiser les pratiques de gestion des données et des systèmes de sécurité.

Présenter les résultats des KPI aux parties prenantes internes (ex. : IT, juridique, directions métiers) et externes (ex. : sous-traitants, partenaires, COMEX), en formulant des analyses stratégiques pour orienter les décisions et prioriser les investissements en sécurité.

Superviser un audit de sécurité et de conformité des systèmes d'information, en définissant le périmètre d'évaluation et les exigences réglementaires (ex. : RGPD, ISO 27001), afin d'identifier les failles de sécurité et les écarts de conformité impactant la protection des données personnelles.

Exploiter les résultats d'un audit de sécurité et de conformité, en analysant les écarts identifiés et en veillant à la mise en œuvre des mesures correctives, afin d'améliorer la protection des données et d'assurer la conformité des dispositifs de sécurité.

Superviser l'application des mesures techniques de sécurité (ex. : chiffrement, segmentation des accès, tests de vulnérabilité) en collaboration avec le RSSI et en s'appuyant sur les standards de cybersécurité (ISO 27001, ANSSI, NIST), afin de garantir une protection efficace des données personnelles et une conformité réglementaire continue.

Surveiller l'évolution des cybermenaces en collaboration avec le RSSI, en mobilisant des outils de détection avancés

(ex : SIEM, EDR) et en effectuant une veille active sur les menaces émergentes, afin d'anticiper et prévenir les risques de sécurité.

Évaluer les incidents de sécurité signalés, en supervisant la mise en œuvre des plans de réponse et des mesures correctives, afin de limiter l'impact sur les données personnelles et de renforcer la capacité de l'organisation à prévenir les violations futures.

Évaluer au préalable les potentiels impacts de causés par des traitements de données sensibles ou à risques pour les droits et libertés des personnes concernées afin d'évaluer le niveau de risques pour les classer par ordre de gravité

Définir des mesures correctives adaptées aux analyses d'impact, en intégrant des solutions spécifiques (ex. : pseudonymisation, anonymisation, renforcement des contrôles d'accès) afin de réduire les risques identifiés et garantir la conformité des traitements.

Cartographier les risques selon leur typologie (financiers, juridiques, réputationnels, opérationnels, etc.) et leur origines (internes : erreurs humaines, falsification, pratiques non conformes, etc. ; et externes : extorsion de données, phishing, intrusion) associés aux traitements de données personnelles, afin d'identifier les priorités.

Évaluer les vulnérabilités associées aux technologies utilisées dans les traitements (ex. : IA, IoT, API), en tenant compte des impacts potentiels sur les droits des personnes concernées, afin de sécuriser l'usage des données et garantir leur conformité.

Prioriser les risques identifiés en fonction de leur criticité et des enjeux de conformité, en appliquant une méthodologie d'évaluation des risques (ex. : Ebios Risk Manager, ISO 27005, etc.), afin d'orienter les actions de remédiation et d'améliorer la maîtrise des traitements de données.

Définir un plan d'actions correctives, en définissant des mesures organisationnelles et techniques adaptées aux risques identifiés, afin d'assurer la sécurité des données et leur conformité ou afin d'atténuer les impacts sur les données personnelles et d'assurer leur mise en conformité avec les exigences réglementaires.

Superviser la mise en œuvre des mesures correctives définies, en coordonnant leur application avec les équipes IT et métiers, en établissant des jalons et des échéanciers adaptés, afin de vérifier leur mise en œuvre, d'évaluer leur efficacité et d'ajuster les actions en fonction des résultats observés.

Concevoir des protocoles de gestion des crises, en définissant des niveaux d'alerte (ex. : niveau de compromission, sites touchés, données touchées, etc.), et en structurant les modalités de signalement et de communication interne et externe, en veillant à ce que les informations et procédures de gestion de crise soient accessibles et compréhensibles pour tous, y compris les personnes en situation de handicap, afin de réduire l'impact des incidents sur l'organisation.

Coordonner les actions correctives en situation de crise, en collaborant avec les équipes internes (IT, juridique, métiers) et en assurant une communication adaptée avec les parties externes (ex. : CNIL, personnes concernées), et en prenant en compte les besoins spécifiques des personnes en situation de handicap ou en difficulté numérique (ex. : communication en langage simplifié, mise à disposition de supports adaptés), afin de limiter les impacts sur les données personnelles et rétablir la sécurité des systèmes.

Evaluer les réponses apportées lors d'une crise (ex. : piratage, perte de données), en analysant les actions correctives mises en œuvre et en identifiant les améliorations nécessaires, afin d'améliorer les protocoles de gestion des crises et garantir une meilleure anticipation des incidents futurs.

Coordonner la mise en œuvre des actions RGPD en mobilisant les parties prenantes internes, en facilitant l'organisation des échanges interservices et en assurant le suivi des actions, afin d'optimiser l'engagement des acteurs et la progression des initiatives de conformité.

Analyser les retours d'expérience sur les actions RGPD réalisées, en identifiant les bonnes pratiques et les points d'amélioration avec les départements métiers (ex. : IT, juridique, opérationnel), afin d'optimiser les processus internes et d'adapter les politiques de conformité aux enjeux opérationnels.

Élaborer une stratégie de communication sur les enjeux et les actions RGPD, en définissant des objectifs et des messages clés pour les publics internes et externes (ex. : collaborateurs, clients, partenaires), afin de renforcer la visibilité des actions de conformité.

Superviser la diffusion des messages RGPD via des canaux adaptés (ex. : intranet, newsletters, plateformes collaboratives) et des formats variés (ex. : vidéos, webinars), en veillant à l'accessibilité des contenus pour tous les publics (ex. : sous-titrage, versions en langage simplifié, compatibilité avec les lecteurs d'écran), afin de maximiser leur impact et renforcer l'engagement des parties prenantes dans la démarche de conformité.

Évaluer l'efficacité des actions de communication, en analysant les retours qualitatifs et quantitatifs (ex. : taux de participation, feedback), afin d'ajuster les stratégies et d'optimiser les campagnes futures.

Concevoir des supports et outils de sensibilisation sur les enjeux de protection des données et les cybermenaces, en

adaptant les messages et formats (ex. : affiches, vidéos, guides pratiques) aux différents publics internes (ex. : équipes RH, marketing, IT), y compris les personnes en situation de handicap, afin d'informer et attirer l'attention sur les bonnes pratiques en matière de protection des données.

Coordonner le déploiement des campagnes de sensibilisation internes sur les enjeux RGPD et la sécurité des données, en utilisant des canaux adaptés (intranet, newsletters, événements), en veillant à ce que ces supports soient accessibles à tous les publics, y compris les personnes en situation de handicap, et

en évaluant leur impact à travers des indicateurs de diffusion et d'engagement, afin de maximiser leur portée et renforcer la culture de la protection des données.

Analyser les besoins de formation en matière de protection des données, en identifiant les compétences à développer pour chaque métier ou département (ex. : juridique, technique, opérationnel), afin de garantir une montée en compétence ciblée.

Concevoir des modules de formation adaptés aux niveaux des collaborateurs (initiation, perfectionnement, expertise), y compris les personnes en situation de handicap, en intégrant des études de cas concrets, afin de faciliter l'apprentissage et l'application des principes RGPD dans les pratiques métiers.

Animer des sessions de formation sur la protection des données, en mobilisant des méthodes pédagogiques adaptées et inclusives (ex. : ateliers pratiques, quiz, jeux de rôle), afin d'assurer l'acquisition des connaissances et des savoir-faire liés aux enjeux RGPD.

Blocs de compétences

RNCP41460BC01 — Auditer et élaborer la politique de conformité et de gouvernance des données

LISTE DE COMPÉTENCES

Cartographier l'ensemble des traitements de données personnelles et sensibles de l'organisation, en identifiant les flux et les acteurs impliqués, en appliquant des techniques de classification des données selon leur sensibilité et en analysant les enjeux de conformité réglementaires et sectoriels (ex. : santé, finance, e-commerce) afin d'établir un diagnostic détaillé des flux de données et des pratiques de traitement

Évaluer la conformité des traitements existants, y compris ceux liés aux technologies émergentes, en analysant les écarts entre les pratiques actuelles et les obligations légales et sectorielles (ex. : santé, finance, e-commerce), afin de qualifier les non-conformités et de prioriser leur gravité selon leur impact sur la conformité de l'organisation.

Produire un rapport de diagnostic détaillé, en hiérarchisant les risques identifiés (ex : risques juridiques, opérationnels, réputationnels) et en formulant des recommandations spécifiques, pour guider la stratégie de mise en conformité de l'organisation.

Créer ou mettre à jour les registres des traitements de données personnelles, en élaborant des fiches descriptives détaillées pour chaque traitement en collaboration avec les responsables métiers, en consolidant les informations requises par le RGPD (ex. : finalités, catégories de données, mesures de sécurité) et en intégrant les spécificités technologiques et métiers de l'organisation (ex. : algorithmes d'IA, protocoles IoT), afin d'assurer une traçabilité complète des activités de traitement et de garantir leur conformité aux exigences réglementaires.

Analyser les contrats en cours avec les sous-traitants et partenaires externes, en vérifiant les clauses liées à la protection des données (ex. : traitement, stockage, partage) et aux engagements des parties prenantes, en mettant en œuvre des processus d'audit contractuel afin de garantir l'application des exigences réglementaires et de sécuriser les échanges de données avec les partenaires.

Gérer les transferts de données hors Union Européenne (UE), en mettant en œuvre les mécanismes juridiques appropriés (ex. : Clauses Contractuelles Types, Binding Corporate Rules) et en assurant le suivi des obligations réglementaires, afin de garantir la conformité et sécuriser les flux transfrontaliers.

Concevoir une politique de gouvernance des données personnelles, incluant des documents opérationnels (ex. : politique de conservation des données, politique de confidentialité, charte RGPD) et des principes clés (ex. : licéité, minimisation, conservation limitée), en collaboration avec les départements métiers (ex. : juridique, IT, marketing) afin d'uniformiser les pratiques de gestion des données et de garantir la conformité au RGPD.

Concevoir des protocoles de gestion des consentements et des préférences, intégrant des mécanismes de preuve (ex : horodatage, journalisation) et de révocation (ex : interface utilisateur dédiée, processus automatisé de suppression), en veillant à leur accessibilité et leur compréhension par l'ensemble des publics concernés, y compris les personnes en situation de handicap, afin de garantir le respect des choix des personnes concernées et leur traçabilité tout au long du cycle de vie des données.

Mettre en place un processus structuré de gestion des demandes d'exercice des droits des personnes concernées

(ex. : droit d'accès, droit d'effacement, droit d'opposition), en intégrant des workflows automatisés (ex. : système de ticketing), en veillant à l'accessibilité des démarches pour tous les publics, notamment les personnes en situation de handicap, et en définissant des indicateurs clés de suivi (ex. : délais de réponse, taux de résolution), afin de garantir un traitement conforme et une traçabilité des demandes dans les délais réglementaires.

Gérer les échanges avec la CNIL lors d'un contrôle ou d'une demande d'information, en rassemblant les éléments de conformité requis et en coordonnant la communication entre les parties prenantes internes et l'autorité de contrôle, afin d'assurer une coopération efficace et démontrer la conformité de l'organisation.

MODALITÉS D'ÉVALUATION

Études de cas (épreuve écrite).

RNCP41460BC02 — Superviser la sécurité des données et des systèmes d'information

LISTE DE COMPÉTENCES

Cartographier les acteurs internes et externes impliqués dans la gestion des données personnelles, en identifiant leurs rôles et responsabilités afin d'assurer une gouvernance alignée avec les objectifs de conformité.

Définir un cadre de gouvernance en collaboration avec les équipes IT et juridiques pour intégrer les principes de Privacy by Design et Privacy by Default dès la conception d'un projet impliquant des traitements de données (ex. : déploiement d'un SIRH, développement d'une application métier, implémentation d'une solution d'IA)

Suivre les politiques de gouvernance et de sécurité à travers des indicateurs clés de performance (KPI) (ex. : taux de résilience aux cybermenaces, conformité des sous-traitants) et des tableaux de bord, en identifiant les écarts pour optimiser les pratiques de gestion des données et des systèmes de sécurité.

Présenter les résultats des KPI aux parties prenantes internes (ex. : IT, juridique, directions métiers) et externes (ex. : sous-traitants, partenaires, COMEX), en formulant des analyses stratégiques pour orienter les décisions et prioriser les investissements en sécurité.

Superviser un audit de sécurité et de conformité des systèmes d'information, en définissant le périmètre d'évaluation et les exigences réglementaires (ex. : RGPD, ISO 27001), afin d'identifier les failles de sécurité et les écarts de conformité impactant la protection des données personnelles.

Exploiter les résultats d'un audit de sécurité et de conformité, en analysant les écarts identifiés et en veillant à la mise en œuvre des mesures correctives, afin d'améliorer la protection des données et d'assurer la conformité des dispositifs de sécurité.

Superviser l'application des mesures techniques de sécurité (ex. : chiffrement, segmentation des accès, tests de vulnérabilité) en collaboration avec le RSSI et en s'appuyant sur les standards de cybersécurité (ISO 27001, ANSSI, NIST), afin de garantir une protection efficace des données personnelles et une conformité réglementaire continue.

Surveiller l'évolution des cybermenaces en collaboration avec le RSSI, en mobilisant des outils de détection avancés (ex. : SIEM, EDR) et en effectuant une veille active sur les menaces émergentes, afin d'anticiper et prévenir les risques de sécurité.

Évaluer les incidents de sécurité signalés, en supervisant la mise en œuvre des plans de réponse et des mesures correctives, afin de limiter l'impact sur les données personnelles et de renforcer la capacité de l'organisation à prévenir les violations futures.

MODALITÉS D'ÉVALUATION

Études de cas (épreuve écrite)

RNCP41460BC03 — Gérer les risques et les crises liés aux traitements de données

LISTE DE COMPÉTENCES

Évaluer au préalable les potentiels impacts de causés par des traitements de données sensibles ou à risques pour les droits et libertés des personnes concernées afin d'évaluer le niveau de risques pour les classer par ordre de gravité

Définir des mesures correctives adaptées aux analyses d'impact, en intégrant des solutions spécifiques (ex. : pseudonymisation, anonymisation, renforcement des contrôles d'accès) afin de réduire les risques identifiés et garantir la conformité des traitements.

Cartographier les risques selon leur typologie (financiers, juridiques, réputationnels, opérationnels, etc.) et leur origines (internes : erreurs humaines, falsification, pratiques non conformes, etc. ;

et externes : extorsion de données, phishing, intrusion) associés aux traitements de données personnelles, afin d'identifier les priorités.

Évaluer les vulnérabilités associées aux technologies utilisées dans les traitements (ex. : IA, IoT, API), en tenant

compte des impacts potentiels sur les droits des personnes concernées, afin de sécuriser l'usage des données et garantir leur conformité.

Prioriser les risques identifiés en fonction de leur criticité et des enjeux de conformité, en appliquant une méthodologie d'évaluation des risques (ex. : Ebios Risk Manager, ISO 27005, etc.), afin d'orienter les actions de remédiation et d'améliorer la maîtrise des traitements de données.

Définir un plan d'actions correctives, en définissant des mesures organisationnelles et techniques adaptées aux risques identifiés, afin d'assurer la sécurité des données et leur conformité ou afin d'atténuer les impacts sur les données personnelles et d'assurer leur mise en conformité avec les exigences réglementaires.

Superviser la mise en œuvre des mesures correctives définies, en coordonnant leur application avec les équipes IT et métiers, en établissant des jalons et des échéanciers adaptés, afin de vérifier leur mise en œuvre, d'évaluer leur efficacité et d'ajuster les actions en fonction des résultats observés.

Concevoir des protocoles de gestion des crises, en définissant des niveaux d'alerte (ex. : niveau de compromission, sites touchés, données touchées, etc.), et en structurant les modalités de signalement et de communication interne et externe, en veillant à ce que les informations et procédures de gestion de crise soient accessibles et compréhensibles pour tous, y compris les personnes en situation de handicap, afin de réduire l'impact des incidents sur l'organisation.

Coordonner les actions correctives en situation de crise, en collaborant avec les équipes internes (IT, juridique, métiers) et en assurant une communication adaptée avec les parties externes (ex. : CNIL, personnes concernées), et en prenant en compte les besoins spécifiques des personnes en situation de handicap ou en difficulté numérique (ex. : communication en langage simplifié, mise à disposition de supports adaptés), afin de limiter les impacts sur les données personnelles et rétablir la sécurité des systèmes.

Evaluer les réponses apportées lors d'une crise (ex. : piratage, perte de données), en analysant les actions correctives mises en œuvre et en identifiant les améliorations nécessaires, afin d'améliorer les protocoles de gestion des crises et garantir une meilleure anticipation des incidents futurs.

MODALITÉS D'ÉVALUATION

Etudes de cas (épreuve écrite)

Mise en situation professionnelle

RNCP41460BC04 — Former et sensibiliser les parties prenantes aux enjeux de protection des données

LISTE DE COMPÉTENCES

Coordonner la mise en œuvre des actions RGPD en mobilisant les parties prenantes internes, en facilitant l'organisation des échanges interservices et en assurant le suivi des actions, afin d'optimiser l'engagement des acteurs et la progression des initiatives de conformité.

Analyser les retours d'expérience sur les actions RGPD réalisées, en identifiant les bonnes pratiques et les points d'amélioration avec les départements métiers (ex. : IT, juridique, opérationnel), afin d'optimiser les processus internes et d'adapter les politiques de conformité aux enjeux opérationnels.

Élaborer une stratégie de communication sur les enjeux et les actions RGPD, en définissant des objectifs et des messages clés pour les publics internes et externes (ex. : collaborateurs, clients, partenaires), afin de renforcer la visibilité des actions de conformité.

Superviser la diffusion des messages RGPD via des canaux adaptés (ex. : intranet, newsletters, plateformes collaboratives) et des formats variés (ex. : vidéos, webinars), en veillant à l'accessibilité des contenus pour tous les publics (ex. : sous-titrage, versions en langage simplifié, compatibilité avec les lecteurs d'écran), afin de maximiser leur impact et renforcer l'engagement des parties prenantes dans la démarche de conformité.

Évaluer l'efficacité des actions de communication, en analysant les retours qualitatifs et quantitatifs (ex. : taux de participation, feedback), afin d'ajuster les stratégies et d'optimiser les campagnes futures.

Concevoir des supports et outils de sensibilisation sur les enjeux de protection des données et les cybermenaces, en adaptant les messages et formats (ex. : affiches, vidéos, guides pratiques) aux différents publics internes (ex. : équipes RH, marketing, IT), y compris les personnes en situation de handicap, afin d'informer et attirer l'attention sur les bonnes pratiques en matière de protection des données.

Coordonner le déploiement des campagnes de sensibilisation internes sur les enjeux RGPD et la sécurité des données, en utilisant des canaux adaptés (intranet, newsletters, événements), en veillant à ce que ces supports soient accessibles à tous les publics, y compris les personnes en situation de handicap, et

en évaluant leur impact à travers des indicateurs de diffusion et d'engagement, afin de maximiser leur portée et renforcer la culture de la protection des données.

Analyser les besoins de formation en matière de protection des données, en identifiant les compétences à développer pour chaque métier ou département (ex. : juridique, technique, opérationnel), afin de garantir une montée en

compétence ciblée.

Concevoir des modules de formation adaptés aux niveaux des collaborateurs (initiation, perfectionnement, expertise), y compris les personnes en situation de handicap, en intégrant des études de cas concrets, afin de faciliter l'apprentissage et l'application des principes RGPD dans les pratiques métiers.

Animer des sessions de formation sur la protection des données, en mobilisant des méthodes pédagogiques adaptées et inclusives (ex. : ateliers pratiques, quiz, jeux de rôle), afin d'assurer l'acquisition des connaissances et des savoir-faire liés aux enjeux RGPD.

MODALITÉS D'ÉVALUATION

Projet professionnel et soutenance orale devant un jury

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Tous les secteurs d'activités et toutes les entreprises, publiques ou privées mais aussi des associations reconnues d'utilité publique, qui gèrent des données de leurs clients, leurs abonnés, leurs salariés quels que soit le statut et la taille de la structure.

TYPE D'EMPLOIS ACCESSIBLES

- Délégué / Déléguée à la protection des données - Data Protection Officer
- Chargé de mission Protection des Données / Chargé de mission RGPD
- Consultant DPO / Consultant RGPD
- Compliance Officer spécialisé en protection des données
- Correspondant / Correspondante informatique et libertés - CIL
- Auditeur / Auditrice en sécurité des systèmes d'information
- Juriste DPO / Juriste Protection des Données Personnelles
- Responsable de la conformité RGPD
- RSSI-DPO (Responsable de la Sécurité des Systèmes d'Information avec mission DPO)

RÈGLEMENTATIONS D'ACTIVITÉ

L'exercice du métier de Délégué à la protection des données n'est pas réglementé mais ce professionnel travaille en s'appuyant sur un cadre réglementaire précis:

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril

2016, relatif à la protection des personnes physiques à l'égard du

traitement des données à caractère personnel et à la libre circulation

de ces données. Il constitue le texte de référence en matière de protection des données personnelles. Ses dispositions sont directement applicables dans l'ensemble des États membres à compter du 25 mai 2018.

- La loi " Informatique et Libertés " du 6 janvier 1978 et la loi du 20 juin 2018 relative à la protection des données personnelles.
- Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO).

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)

Élevée (4/5)

Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.

Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 893 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	L5X91 — Juristes et avocats · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	7 644
Jugés difficiles à recruter	42 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	L5X91 — Juristes et avocats M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Pour accéder à la formation menant à la certification professionnelle "Délégué à la protection des données (DPO)", ainsi qu'aux blocs de compétences constitutifs du titre, les candidats doivent satisfaire aux conditions préalables suivantes : être titulaire d'une certification professionnelle ou d'un diplôme de niveau 6 ou être titulaire d'un niveau 5 et justifier de minimum 1 an d'expérience dans l'informatique ou le droit

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, VAE

2 professionnels en activité dans l'informatique ou le droit dont 1 est président de jury, externes au réseau Doranco
1 représentant du certificateur

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	8 684 €
Selon la branche	7 500 € – 8 789 €
Prise en charge	Branches concernées
8 684 €	Valeur par défaut · 205 branches
8 789 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie, CPNEFP ICGV entreprises de la viande
8 668 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
8 752 €	CPNEFP dans les établissements d'enseignement privés sous contrat
8 700 €	CPNEFP des jardineries et graineteries
8 583 €	CPNEFP Commerce à distance
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	27/10/2025
-------------------------	------------

Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	27/10/2028
Date de dernière délivrance possible	26/10/2032

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2024	30	0	45 %	—
2023	11	0	100 %	86 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP35086

CORRESPONDANCES (PAR BLOCS)

RNCP35086, RNCP36448, RNCP37346, RNCP38106, RNCP38585, RS5144, RS5333, RS5569

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/41460/>